Technische Hochschule Ingolstadt

Fakultät Informatik

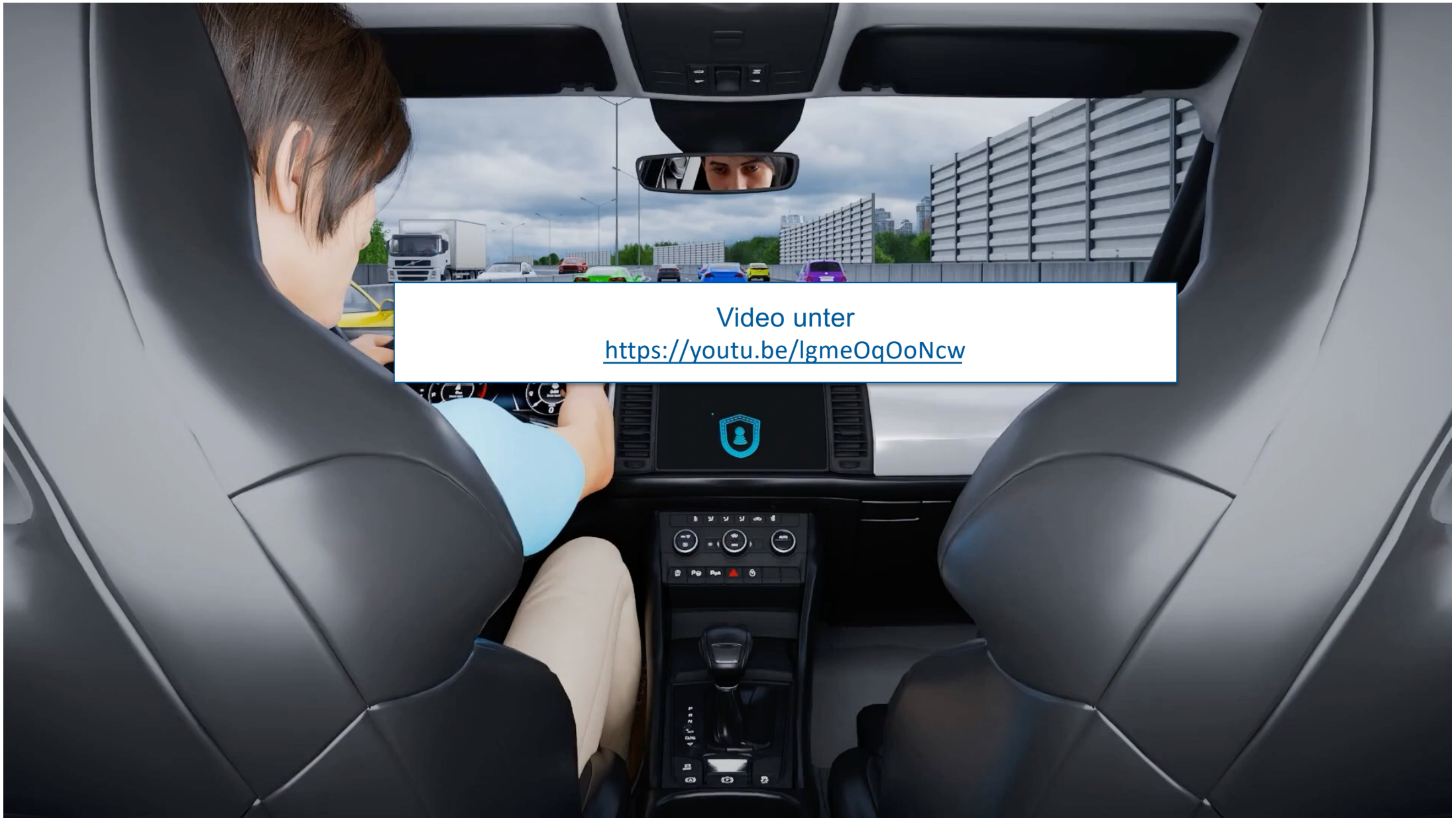
Überwachung von Fahrzeugen im Feld – Bericht aus dem Forschungsprojekt SELFY

Prof. Dr.-Ing. Hans-Joachim Hof

Technische Hochschule Ingolstadt

04.05.23

- **UNECE R155 fordert Cybersicherheit für Fahrzeuge im Betrieb, dazu gehört z.B.**
  - Intrusion Detection
  - Umfeldbeobachtung
  - Incident Management
  - Security Updates
  - Sicherer Zugriff auf Fahrzeugdaten


Video unter
https://youtu.be/lgmeOqOoNcw

VSOC in SELFY

Forschungsfragestellungen

- **Wie können Security Vorfälle in einem CCAM Umfeld detektieren werden?**
- **Welche Arten von Angriffe kann das SELFY VSOC detektieren?**
- **Wie kann auf Security-Vorfälle reagiert werden?**
- **Welche Funktionen des SELFY VSOC können inwieweit automatisiert werden?**
- **Welche Daten benötigt das SELFY VSOC?**

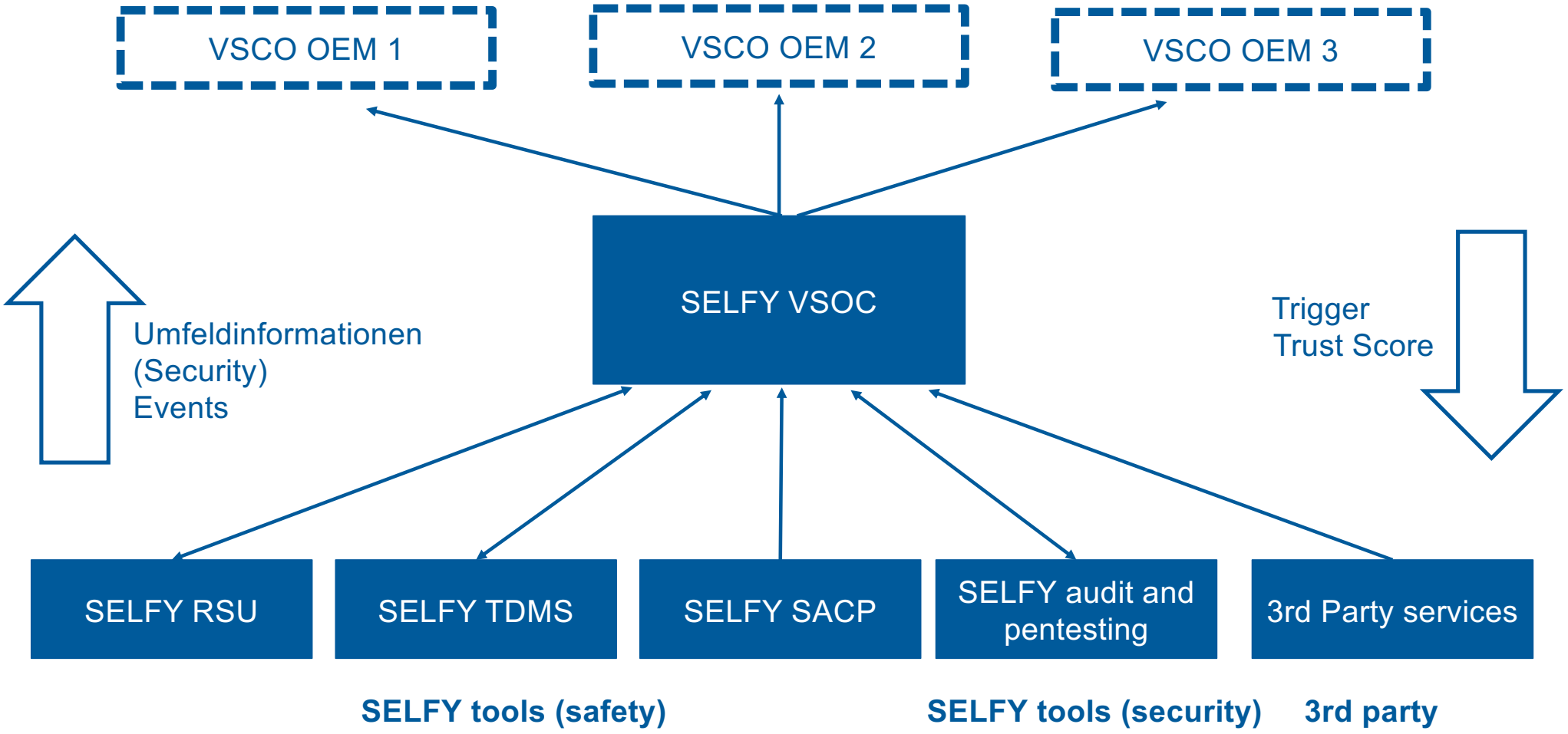
SELFY

Grundsätzlicher Ansatz

- **SELFY Toolbox: Vielzahl von Mechanismen für Safety & Security**
  - Können nach Bedarf zusammengestellt werden
  - Können nach Bedarf erweitert werden
- **Lokale Reaktionsmechanismen und zentrale Reaktionsmechanismen**
  - Lokal: schnelle, automatische Reaktion einzelner Fahrzeuge
  - Zentral: Koordinierte Reaktion einer Gruppe von Fahrzeugen, Änderung von Netzwerkparametern
- **VSOC als zentraler Koordinator für SELFY Toolbox**
  - Direkter Trigger für Aktionen
  - Änderung Trust Score (lokal, regional, global)

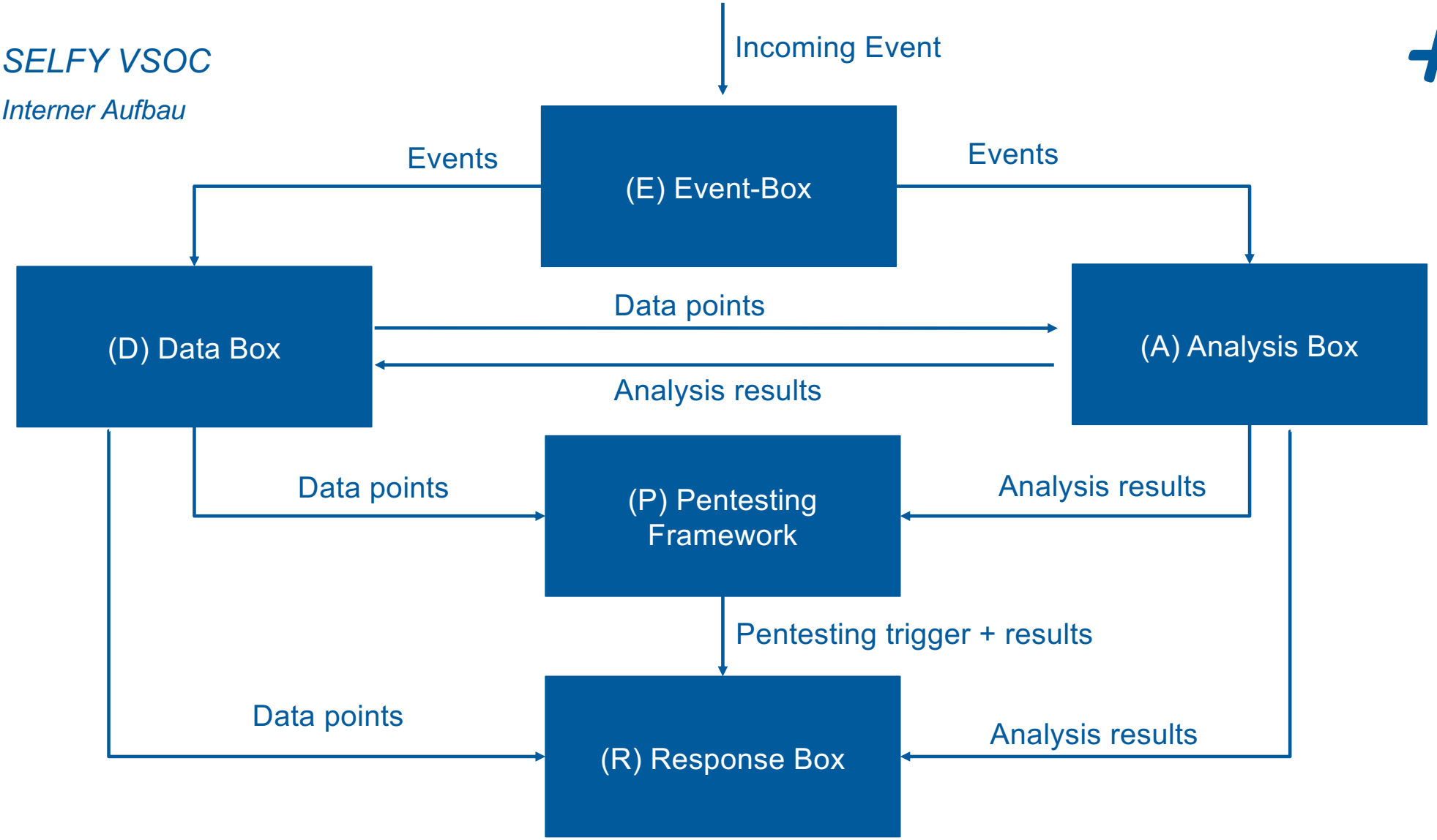
SELFY VSOC

Architektur



SELFY VSOC

Interner Aufbau



SELFY VSOC

E-Box & D-Box

- **E-Box: Verarbeitung von Events von SELFY Tools**
  - Datensammlung
  - Klassifikation Events
  - Verifikation Events
- **D-Box: Speicherung und Transformation Daten**
  - Speicherung Rohdaten
  - Indexerstellung
  - Speicherung Log-Dateien
  - Speicherung Uptane Images
  - Speicherung 3rd Party Information
  - Update Sicherheitsmetriken

SELFY VSOC

A-Box & R-Box

- **A-Box: Analyse der Events und gespeicherte Daten**
  - Datenkorrelation
  - Dashboard
  - Packet Inspection
  - Insbesondere: Erkennung Bedrohungen UNECE R155 Annex 5

- **R-Box: Reaktion auf Analyseergebnisse**
  - Alarmierung
  - Trigger/Action auslösen
  - Trust Score anpassen und verbreiten

Mögliche Trigger/Actions

- **SELFY Audit/Pentesting Tool wird ausgelöst**
- **Software Update wird getriggert**
- **Aktivierung Isolation Mode für erkannte Bedrohung**
- **Aktivierung Safe and Secure Mode bei unbekannter Bedrohung**
- **Zusammenspiel lokale/globale Security-Mechanismen**

Zusammenfassung

- **SELFY bietet eine Toolbox mit verschiedenen Safety&Security Tools**
- **SELFY VSOC für zentrale Koordination Security, unabhängige lokale Reaktion**
- **SELFY VSCO ist ein Meta VSOC, kann zusätzlich zu OEM VSOC eingesetzt werden**

Herzlichen Dank für die Aufmerksamkeit

Prof. Dr.-Ing. Hans-Joachim Hof
Technische Hochschule Ingolstadt
hof@thi.de

Linkedin 👇

www.selfy-project.eu